Opis predmetu zákazky, technické požiadavky

Zavedenie služieb Hardware Secure Module (HSM) as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania – služby Vládneho Cloudu:

* Multitenantná služba HSM s priamym prístupom pre manažment kľúčov a PKI
* Multitenantná služba HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovania

# OBSAH

[OBSAH 2](#_Toc113528608)

[1 Všeobecné informácie 4](#_Toc113528609)

[1.1 Základné ciele projektu HSM as a Service. 4](#_Toc113528610)

[1.1.1 Hardware Secure Module (HSM) as a Service služba: 4](#_Toc113528611)

[1.1.2 Služba Multi-tenant HSM so službou HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovanie: 5](#_Toc113528612)

[1.2 Popis súčasného stavu - IaaS 5](#_Toc113528613)

[1.2.1 Prevádzka IaaS Vládneho Cloudu 6](#_Toc113528614)

[1.3 Definície, akronymy, skratky a vymedzenie pojmov 6](#_Toc113528615)

[1.4 Predmet 9](#_Toc113528616)

[1.5 Trvanie a realizácia predmetu zákazky, harmonogram projektu 9](#_Toc113528617)

[1.6 Miesto realizácie 11](#_Toc113528618)

[1.7 Požadované časti dodávky 11](#_Toc113528619)

[1.7.1 Analýza a návrh riešenia 12](#_Toc113528620)

[1.7.2 Implementácia riešenia 12](#_Toc113528621)

[1.7.3 Nasadenie do pilotnej prevádzky 12](#_Toc113528622)

[1.7.4 Pilotná prevádzka systému 13](#_Toc113528623)

[1.7.5 Licencie pre všetky súčasti riešenia 13](#_Toc113528624)

[1.7.6 Školenia a konzultácie 13](#_Toc113528625)

[1.7.7 Dokumentácia 13](#_Toc113528626)

[1.7.8 Prevod a prechod duševného vlastníctva podľa aktuálnych pravidiel MIRRI 13](#_Toc113528627)

[1.7.9 Podpora a údržba prevádzky 14](#_Toc113528628)

[1.7.10 Integrácia s CSP portálom Vládneho Cloudu 15](#_Toc113528629)

[1.7.10.1 Očakávaná funkcionalita od integrácie HSM s priamym prístupom s CSP portálom 15](#_Toc113528630)

[1.7.10.2 Očakávaná funkcionalita pre HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovanie 15](#_Toc113528631)

[1.7.11 Bezpečnostný projekt 16](#_Toc113528632)

[2 Všeobecné požiadavky 17](#_Toc113528633)

[2.1 Legislatívne požiadavky na riešenie 17](#_Toc113528634)

[2.2 Architektonické požiadavky 17](#_Toc113528635)

[*2.2.1* *Uplatnenie EA architektonického rámca* 18](#_Toc113528636)

[*2.2.2* *Stavebné bloky architektúry* 18](#_Toc113528637)

[*2.2.3* *Ďalšie požiadavky na architektúru riešenia* 18](#_Toc113528638)

[2.3 Požiadavky na Bezpečnosť 18](#_Toc113528639)

[2.4 Projektové požiadavky 18](#_Toc113528640)

[2.4.1 Projektové riadenie 18](#_Toc113528641)

[2.4.2 Dokumenty projektového riadenia 19](#_Toc113528642)

[2.4.3 Záruka na všetky komponenty služby HSM as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania. 21](#_Toc113528643)

[3 Detailné požiadavky na predmet zákazky 22](#_Toc113528644)

[3.1.1 Úrovne služieb Hardware Secure Module (HSM) as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania – služby Vládneho Cloudu 22](#_Toc113528645)

[3.2 Požiadavky na Multi-tenantnú službu HSM s priamym prístupom pre Key Management a PKI 22](#_Toc113528646)

[3.3 Požiadavky služieb Centrálneho manažmentu kľúčov a Transparentného Šifrovania s využitím HSM na správu kľúčov. – služby Vládneho Cloudu 24](#_Toc113528647)

[4 Akceptačné konanie 26](#_Toc113528648)

[4.1 Metódy akceptácie 27](#_Toc113528649)

# Všeobecné informácie

Tento dokument popisuje požiadavky na dodávku riešenia: Zavedenie služieb Hardware Secure Module (HSM) as a Service – služby Vládneho cloudu. Toto riešenie bude pozostávať z dvoch častí. Prvé je multitenantná služba HSM s priamym prístupom pre manažment kľúčov a PKI . Druhou je multitenantná služba HSM s centrálnou službou Manažmentu kľúčov a transparentného šifrovania.

Požiadavky sú zostavené do častí a tvoria ucelené riešenie:

* HSM hardware
* HSM licencie a Supporty
* Dodanie HSM software – Manažér Kľúčov, software pre servery/ kontainery. (V rámci riešenia)
* Implementačné práce
* Podpora riešenia POC
* Integrácia s CSP portálom
* Zaškolenie personálu / Dokumentácia

## Základné ciele projektu HSM as a Service.

Hardware Secure Module (HSM) as a Service služba vládneho cloudu, podľa štúdie uskutočniteľnosti bude určená pre organizácie VS pre účely:

* Migrácie existujúcich ISVS do vládneho cloudu.
* Prípravy nových ISVS s využitím HSM služieb a transparentného šifrovania.
* Podpora nových projektov a implementácie v prostredí Vládneho Cloudu s podporou služieb HSM.
* Rozšírenie existujúcich ISVS o služby HSM a služby transparentného šifrovania.

Projekt Hardware Secure Modul (HSM) bude dodaný v plnom súlade so štúdiou uskutočniteľnosti, ktorá je uverejnená na nasledovnej linke: <https://metais.vicepremier.gov.sk/detail/Projekt/121fd23d-3b11-4d86-9faa-1e6c71b53ce6/cimaster?tab=basicForm> (P\_SU-PaaS-su\_111\_PaaS\_MVSR\_16012018\_v111.pdf)

### Hardware Secure Module (HSM) as a Service služba:

* Lokálne hardware riešenie
  + jednoduchá implementácia v prostredí vládneho cloudu.
  + Tamper proof riešenie, bez možnosti extrakcie certifikátov.
* Multi-tenantné riešenie
  + Riešenie vhodne pre nasadenie a využitie viacerými klientami a organizáciami štátnej správy.
  + podpora až 100 separátnych tenantov/separátnych organizácií(na jednom HSM), ktorý sú absolútne oddelení
* Licencovanie na základe počtov partícií a počtu klientov, ktorý budú pristupovať na službu HSM.
* Možnosť rýchleho nasadenia pre potreby zákazníkov Vládneho Cloudu Ministerstva Vnútra SR.
* Možnosť škálovateľnosti pri veľkom dopite po tejto službe.
* Možnosť výberu a definície HSM clusteringu pre vysokú dostupnosť formou Active/Active alebo
* Active/Standby.

V súvislosti s uvedeným požadujeme, aby riešenie HSM as a service:

* Prinieslo nové moderne riešenie, ktoré predstavuje technologický najbezpečnejšie riešenie pre funkcionalitu general purpose HSM(Multi-Tenant).
* Prinieslo možnosti škálovateľnosti a rýchleho nasadenia pre potreby nových tenantov.
* Zjednodušilo proces implementácie a manažmentu HSM as a service služby.
* Prinieslo ušetrenie nákladov na ľudské zdroje a službu v porovnaní s plne dedikovaným riešením.
* Prinieslo redundantne riešenie s vysokou dostupnosťou.
* Prinieslo možnosť funkcionality „Split of Responsibilites“ a prideľovania práv pre jednotlivých tenantov.
* Prinieslo možnosť využívať HSM pre tenantov aj mimo vládneho cloud prostredia (Rent HSM pre on-prem).
* Podpora bring your own key. Tenant si priamo do HSM nahrá kľuč z vlastného systému.

### Služba Multi-tenant HSM so službou HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovanie:

* Lokálne softwarové riešenie s integráciou na HSM
  + jednoduchá možnosť implementácie v prostredí vládneho cloudu
* Multi-tenant riešenie
  + Riešenie poskytuje možnosť implementácie dedikovanej domény separátne pre každého zákazníka Vládneho Cloudu MVSR
* Licencovanie na základe počtu Domén a systémov, ktoré majú byt zašifrované
* Možnosť rýchleho nasadenia pre potreby zákazníkov Vládneho Cloudu Ministerstva Vnútra SR.
* Možnosť šifrovania existujúcich systémov „za behu“, bez nutnosti ich odstavenia.
* Možnosť centrálneho manažmentu kľúčov pre jednotlivé domény.
* Bezpečnosť kľúčov je zabezpečená zariadením HSM

V súvislosti s uvedeným požadujeme, aby riešenie centrálneho manažmentu kľúčov a transparentného šifrovania s integráciou na službu HSM poskytovalo nasledovné benefity:

* Prinieslo nové moderne riešenie, ktoré predstavuje technologický najlepšie riešenie pre funkcionalitu transparentného šifrovania.
* Prinieslo možnosti škálovateľnosti a rýchleho nasadenia pre potreby nových tenantov.
* Zjednodušilo proces implementácie a manažmentu služby transparentného šifrovania
* Prinieslo ušetrenie nákladov na ľudské zdroje a službu v porovnaní s plne dedikovaným riešením
* Prinieslo redundantne riešenie s vysokou dostupnosťou.
* Prinieslo možnosť funkcionality „Split of Responsibilites“ a prideľovania práv pre jednotlivých tenantov
* Integrácia na existujúci portál MVSR Vládneho Cloudu.

## Popis súčasného stavu - IaaS

V súlade so schváleným strategickým materiálom „Návrh centralizácie a rozvoja dátových centier v štátnej správe“, ktorý bol vládou SR schválený dňa 21.5.2014 bola postupne od roku 2015 budovaná cloudová infraštruktúra poskytujúca služby odberateľom cloudových služieb.

V rámci Služieb IaaS nie je dostupná multi-tenantná HSM as a Service. Pokiaľ boli implementované HSM služby v rámci služby vládneho cloudu MVSR, tak iba ako dedikovane riešení, ktoré nie je možné zdieľať s inými tenantami (konzumentami) Vládneho Cloudu. Úlohou tohto obstarávania je definovať a implementovať služby HSM as a service, pre použitie viacerých subjektov, ktoré konzumujú služby vládneho cloudu a majú potreby pre využitie služieb HSM as a service v multi-tenant režime.

To isté platí pre službu centrálneho manažmentu kľúčov (Key Management) a transparentného šifrovania.

Táto služba nie je štandardnou službou Vládneho Cloudu Ministerstva vnútra SR. Úlohou tohto obstarávania je definovať a implementovať služby manažmentu kľúčov (Key Management) a transparentného šifrovania pre použitie viacerých subjektov, ktoré konzumujú služby vládneho cloudu. Neoddeliteľnou súčasťou je aj funkcia automatizácie pri vytváraní prístupu k tejto službe cez portál MVSR Vládneho Cloudu (CPS).

### Prevádzka IaaS Vládneho Cloudu

Prevádzka IaaS Vládneho Cloudu je v súčasnosti zabezpečovaná pracovníkmi MV SR pre obidve lokality (DC Kopčianska, DC Tajov), v ktorých je IaaS Vládneho Cloudu nasadený.

MV SR zabezpečuje prevádzku a podporu pracovníkmi, vrátane procesu implementácie projektov na úrovni IaaS.

Poskytované sú aj služby podpory cez Call Centrum MV SR, ako aj prostredníctvom implementovaného systému Service Desk, ktorý je dostupný pre odberateľov a kde je možné evidovať jednotlivé incidenty.

Zabezpečenie prevádzky infraštruktúry IaaS pracovníkmi MV SR a poskytovanie príslušných služieb vrátane riešenia incidentov je v súčasnosti v režime 15/5 od 7:00-22:00hod.

Zabezpečenie procesu správy a prevádzky poskytovania služieb IaaS je v režime 8/5.

Dostupnosť všetkých služieb IaaS vládneho cloudu je zabezpečená v režime 24/7 na úrovni 99.5%.

Služby IaaS, ktoré Vládny Cloud v súčasnosti poskytuje sú popísané v MetaIS ako aj na stránke https://www.sk.cloud/ v katalógu služieb.

## Definície, akronymy, skratky a vymedzenie pojmov

Tabuľka č.1 Prehľad definície použitých pojmov a skratiek uvedených v dokumente

|  |  |
| --- | --- |
| **Pojem / skratka** | **Vysvetlenie** |
| API | Application programming interface (rozhranie pre programovanie aplikácií) |
| HSM | Hardware Secure Module |
| Tenant | Entita, jedinec, organizácia |
| DB | Databáza |
| EA | Enterprise Architecture |
| PKI | Public Key infrastrucutre |
| ACL | Access control list |
| HW | Hardware |
| SW | Software |
| LB | Load Balancer |
| RSA | Rivest–Shamir–Adleman |
| Gbps | Gigabits per second |
| IP | Internet protocol |
| SNMP | Simple Network Management Protocol |
| Syslog | is a standard for message logging |
| FIPS | Federal Information Processing Standard |
| PKCS | Public Key Cryptography Standards |
| CSP | Cryptographic Service Provider |
| CPS | Cloud provisioning system |
| CNG | Cryptography Next Generation API from Microsoft |
| EÚ | Európska únia |
| GUI | Graphical User Interface (Grafické používateľské rozhranie) |
| IKT | Informačno-komunikačné technológie |
| IS | Informačný systém |
| ISVS | Informačný Systém Verejnej Správy |
| IT | Informačné Technológie |
| MF SR | Ministerstvo Financií Slovenskej republiky |
| SAML2 | Security Assertion Markup Language 2.0 |
| SLA | Service-level agreement, (Dohoda o poskytovaných službách) |
| SR | Slovenská Republika |
| SSO | Single Sign On |
| TOGAF | The Open Group Architecture Forum, (štandard pre definovanie enterprise architektúry) |
| UML | Unified Modeling Language; zjednotený modelovací jazyk |
| WS | Web Service (Webová služba) |
| XML | eXtensible Markup Language, (rozšíriteľný značkovací jazyk) |
| CE | European Conformace |
| UL | Underwriters Laboratories |
| FCC | Federal Communications Commission |
| AES | Advanced Encryption Standard |
| Triple DES | Tripel Data Encryption Standard |
| ECC | Elliptic Curve Cryptography |

Tabuľka č.2 Vymedzenie pojmov pre HSM as a Service službu a služby transparentného šifrovania:

|  |  |
| --- | --- |
| **Pojem / skratka** | **Vysvetlenie** |
| Split of responsibilites | Predstavuje koncept, kde sú definované viaceré role a každá ma iné právomoci. |
| Remote Backup (RBS) | RBS poskytuje služby vzdialeného backupu pre viacero HSM zariadení a partii z centrálnej lokality. |
| Signing functionality | Funkcia podpisu v rámci General Purpose HSM slúži na podpis transakcii a aktivít v rámci aplikácii Vládneho Cloudu. |
| Secure transport mode | Je to režim bezpečného prevozu, kedy je zabezpečené, že zariadenie nebolo kompromitované počas prevozu. |
| HSM partition | Predstavuje chránené a uzavreté prostredie, kde môžu aplikácie ukladať a používať kryptografické údaje. |
| Aplikácia | Softvér, ktorý používa inštanciu služby prostredníctvom väzby služby. |
| Manažované služby (Managed Services) | Sú definované ako služby integrovateľné s riešením HSM as a Service pomocou rozhraní API a umožňujú koncovým používateľom poskytovať na požiadanie rezervované zdroje a poverenia (credentials). |
| API sprostredkovateľa služby | API sprostredkovateľa služby definuje HTTP rozhranie medzi katalógom služieb platformy a sprostredkovateľmi služby. |
| Mikroslužby | Opisujú návrhový prístup pre samotnú tvorbu aplikácie, ktorý rozdeľuje aplikáciu na sériu samostatných procesov, nasadených nezávisle a prepojených prostredníctvom servisných rozhraní. Koncepcia spočíva v tom, že mikro služby v aplikácii by mali byť navrhnuté tak, aby implementovali určitú konkrétnu oblasť funkcie konkrétny proces. |
| Key management | Centrálny manažment šifrovacích kľúčov na potrebu služieb v rámci Vládneho Cloudu. |
| HSM Partícia | Oddelený filesystem pre správu tokenov viditeľných pre skupinu klientov v rámci tenanta. |

Vymedzenie predmetu obstarávania

## Predmet

Predmet verejného obstarávania pozostáva s nasledovných častí:

* HSM hardware
* HSM licencie a support (Podpora od vendora)
* Dodanie nadstavbového HSM software – Manažér Kľúčov, software klientskych staníc. (V rámci riešenia)
* Implementačné práce
* Automatizácia deploymentu tenantov na HSM (vytvorenia tenantov)
* Podpora riešenia
* Zaškolenie personálu / Dokumentácia

## Trvanie a realizácia predmetu zákazky, harmonogram projektu

Plnenie predmetu zákazky

* Plnenie začína dňom nadobudnutia účinnosti Zmluvy o dielo podpísanej s úspešným uchádzačom.
* Obstarávateľ požaduje zaradenie pilotnej prevádzky nasadenia služby HSM as a Service v trvaní 6 týždňov v priestoroch obstarávateľa pred nasadením do produkcie. V uvedenom čase požadujeme súčinnosť zhotoviteľa.
* Celková dĺžka realizačnej fázy predmetu zákazky je do 6 mesiacov od začiatku účinnosti zmluvy. Toto obdobie môže byť predĺžené po dohode oboch strán. Za ukončenie realizačnej fázy predmetu zákazky sa rozumie situácia, kedy zadávateľ prevezme a akceptuje predmet projektu od zhotoviteľa preberacím a akceptačným protokolom.
* Súčasne požadujeme zohľadniť nasledovné princípy plánovania aktivít pre realizáciu predmetu zákazky:
  + Primeraná dĺžka prípravnej a analytickej fázy (od 10% do 30% trvania implementačnej fázy),
  + Využiť paralelnú implementáciu komponentov/subsystémov,
  + Primerané testovanie u zákazníka s rozložením na iterácie (od 10% do 40% trvania implementačnej fázy, minimálne 3 iterácie)

Nasledujúca tabuľka uvádza Harmonogram a požadované termíny realizácie jednotlivých činností. Údaje v stĺpci „Plánovaný začiatok“ a „Plánovaný koniec“ vyjadrujú mesiace od začiatku projektu. Údaj v stĺpci „Trvanie“ uvádza trvanie danej činnosti v mesiacoch. Trvanie činnosti je dané intervalom od začiatku mesiaca uvedeného v stĺpci „Plánovaný začiatok“ až po koniec mesiaca v stĺpci „Plánovaný koniec“.

|  |  |  |  |
| --- | --- | --- | --- |
| **Názov činnosti** | **Plánovaný začiatok** | **Plánovaný koniec** | **Trvanie** |
| Analýza a návrh riešenia | 1M | 1M | 1M |
| Špecifikácia požiadaviek IKT | 2M | 2M | 1M |
| Implementácia | 3M | 3M | 1M |
| Integrácia s CPS portálom | 3M | 4M | 1M |
| Testovanie riešenia | 3M | 4M | 1M |
| Nasadenie do pilotnej prevádzky | 4M | 5M | 1M |
| Pilotná prevádzka systému | 4M | 5.5M | 1M |
| Produkčná prevádzka (štart a zvýšená podpora) | 6M | 6M | 1M |
| Podpora produkčnej prevádzky (SLA) | 7M | 66M | 60M |

Uchádzač je vo svojej ponuke povinný predložiť detailný časový harmonogram plnenia predmetu zákazky, ktorý bude neoddeliteľnou súčasťou zmluvy, ktorý bude členený na jednotlivé činnosti (1 až 7) pričom každú činnosť rozdelí na ucelené čiastkové plnenia (čiastkové plnenia projektu). Každú činnosť projektu, resp. čiastkové plnenia musí uchádzač vo svojej ponuke ohraničiť termínom predpokladaného začiatku a ukončenia ním definovaných činností alebo čiastkových výstupov projektu. Činnosti potrebné pre zhotovenie jednotlivých dodávok projektu musia mať vyznačenú vzájomnú logickú a časovú nadväznosť. Termíny ukončenia činností alebo odovzdania čiastkových výstupov projektu budú považované za míľniky projektu a budú brané ako termíny slúžiace na akceptáciu čiastkových plnení. Časový harmonogram bude obsahovať zoznam hlavných míľnikov projektu a zoznam a termíny dodania jednotlivých dodávok projektu.

Navrhne plán jednotlivých dodávok a produktov predmetu zákazky z pohľadu upresnenia platobných míľnikov maximálne v členení na

* HSM hardware, HSM licencie a suport, Dodanie HSM software (V rámci riešenia), Dodanie licencií centrálneho manažmentu kľúčov (Key management) a pre riešenie transparentného šifrovania.
* Implementačné práce
* Podpora riešenia
* Zaškolenie personálu / dokumentácia
* Bezpečnostný projekt podľa vyhlášky č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu a iných prislúchajúcich vyhlášok a zákonov. Obstarávateľ prejaví súčinnosť na vytváraní Bezpečnostného projektu.

Uchádzač jednotlivé čiastkové výstupy plnenia projektu v harmonograme plnenia predmetu zákazky v ponuke aj ocení (vyjadrí v EUR bez DPH aj v EUR s DPH).

## Miesto realizácie

Jednotlivé komponenty riešenia musia byť prevádzkované v prostredí IaaS DC MV SR, ktoré boli realizované v rámci národného projektu „IKT infraštruktúry pre poskytovanie IaaS služieb v Datacentre MV SR“ vybaveného modernou IKT infraštruktúrou. Infraštruktúra DC spĺňa všetky požiadavky na výpočtový výkon, úložnú kapacitu, bezpečnosť a zabezpečenie prevádzky, dostupnosť a operačné prostredie.

Z pohľadu typu služby musí ísť o privátne/ on-prem nasadenie služby HSM as a service a služby transparentného šifrovania.

**Požiadavky na využitie existujúcej IKT infraštruktúry Vládneho Cloud, IaaS a priestoru v datacenterách.**

Dodávateľ bude poskytovať podporné a prevádzkové služby pre ním dodávané riešenie v rozsahu:

* správu HSM infraštruktúry pre novo budované systémy podľa tohto zadania,
* správa služby centrálneho manažmentu kľúčov a transparentného šifrovania pre nových a existujúcich zákazníkov
* poskytovania služieb vrátane poradenských služieb pre HSM a jeho integráciu,
* poskytovania služieb vrátane poradenských služieb pre riešenie transparentného šifrovania
* migrácie kľúčov z existujúcich služieb HSM do služieb HSM Vládneho Cloudu,
* nastavovania, backupovanie, monitorovania HSM služieb a služby transparentného šifrovania,
* riadenia zmien a optimalizácie HSM služby a služby transparentného šifrovania,.
* Aktualizácia jednotlivých komponentov celého riešenia na výrobcom podporovanú konfiguráciu

Obstarávateľ požaduje poskytnúť detailné informácie (guideline) o tom, ako bude budúci dodávateľ HSM služby postupovať v oblasti implementácie a integrácie služby HSM do prostredia Vládneho Cloudu. (Stratégia migrovania).

Dodávateľ musí byť schopný podporiť prevádzku a správu v úrovni odborných znalostí úrovne L1-L2-L3, v oblasti záťaže v „cloudovej oblasti“, ako aj správu a dodržovanie SLA.

Obstarávateľ požaduje od uchádzača návrh a dodávku nástrojov potrebných na správu HSM a služby centrálneho manažmentu kľúčov a transparentného šifrovania, a odporúčania na samoobslužný portál potrebný pre správu HSM služby MV SR.

## Požadované časti dodávky

V závislosti od fázy projektu a časti predmetu obstarávania požadujeme dodať nasledovné súčasti riešenia:

* Pilotná prevádzka systému
* Analýza a návrh riešenia,
* Implementácia riešenia
* Školiace materiály pre užívateľov (tenantov) – video návody, web, FAQ,
* Dokumentácia k implementácií
* Licencie pre všetky súčasti riešenia
* Záruka na všetky softvérové súčasti a riešenia HSM as a Service
* Podpora prevádzky
* Bezpečnostný projekt a bezpečnostné smernice
* Integrácia s CPS portálom
* Riadenie projektu za pomoci projekt manažérov

### Analýza a návrh riešenia

Keďže požadované služby nie sú dostupné v prostredí Vládneho Cloudu, je dôležité analyzovať potreby jeho využitia a pripraviť všetky potrebné materiály na možnosť implementácie.

Očakávané výstupy sú nasledovné:

* High level architektúra
* Low level architektúra
* Návrh a popis dátových tokov
* Popis integrácie s internými manažment a monitoring systémami
* Návrh a popis umiestnenia v sieti vládneho cloudu
* Návrh a popis integrácie s portálom CSP
* Popis provisioning flowov vytváraní partícií/ domén a prístupu pre tenantov

### Implementácia riešenia

Požadujeme, aby zhotoviteľ popísal detailný postup nasadenia služby HSM as a Service na základe požiadaviek. Pričom výstupom bude:

* Funkčná služba HSM as a Service
* Funkčná backupová služba pre službu HSM as a Service
* Funkčná služba výkazov (reporting),
* Funkčná služba centrálneho manažmentu kľúčov
* Funkčná služba transparentného šifrovania
* Funkčná backupová služba pre služby transparentného šifrovania a centrálneho manažmentu kľúčov

### Nasadenie do pilotnej prevádzky

Požadujeme, aby zhotoviteľ na základe detailného postupu nasadenia služby HSM as a Service a služby transparentného šifrovania a ostatných častí riešenia nasadil riešenie do produkčného prostredia a zrealizoval potrebné kroky na zahájenie pilotnej prevádzky systému.

### Pilotná prevádzka systému

Počas pilotnej prevádzky (v trvaní podľa Harmonogramu projektu dodaného úspešným uchádzačom) sa požaduje možnosť každodennej konzultácie cez komunikačné prostriedky (telefón, email) v čase od 8:00 do 16:00 v pracovné dni, a podľa dohody realizácia projektových a pracovných stretnutí v priestoroch objednávateľa.

Pilotná prevádzka realizuje prevádzku plnej funkcionality riešenia, kde obstarávateľ si určí ohraničenie používateľa/ov služby HSM as a Service a služby transparentného šifrovania.

### Licencie pre všetky súčasti riešenia

Riešenie bude obsahovať detailný prehľad licencií a suportov, ktoré sú potrebné pre realizáciu tohto projektu. Dodávateľ musí popísať licencie, ktoré budú dodané dodávateľom. Tak isto bude potrebné popísať, aké licencie a technické prostriedky budú dodané Obstarávateľom.

### Školenia a konzultácie

V rámci realizácie projektu Obstarávateľ požaduje navrhnutie a vykonanie nasledovných školení v priestoroch Obstarávateľa a to pre multitenantná služba HSM s priamym prístupom pre manažment kľúčov a PKI. Tak isto aj pre multitenantná služba HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovania:

* Školenie pre používateľov v potrebnom rozsahu
* Školenie pre administrátorov v potrebnom rozsahu

Školenie, ktoré zahŕňa integráciu s CSP portálom bude v zodpovednosti dodávateľa integrácie s CSP portálom.

Výstupom sú školenia, školiace materiály a potvrdenia o absolvovaní pre účastníkov školenia

### Dokumentácia

Obstarávateľ požaduje od zhotoviteľa dodať nasledovnú dokumentáciu:

* Prevádzkovú dokumentáciu
* Dokumentáciu k Architektúre riešenia
* Používateľskú dokumentáciu (Súčasť integrácie s CSP portálom)
* Bezpečnostný projekt podľa súčasných inštrukcií od MIRRI.

Zhotoviteľ poskytne uvedenú dokumentáciu 1x na digitálnom médiu (CD alebo DVD) a 1x v tlačenej forme.

### Prevod a prechod duševného vlastníctva podľa aktuálnych pravidiel MIRRI

Ak bude riešenie vyžadovať na vybudovanie služieb HSM as a Service a služby transparentného šifrovania aj licenčný softvér obstarávateľ požaduje, aby zhotoviteľ dodal potrebné licencie a licenčné kľúče tak, aby bolo riešenie v súlade s požadovanými licenčnými podmienkami dodávaných príslušných komponentov. Súčasne, v prípade použitia licencovaného alebo opensource softvéru, uchádzač uvedie presný názov a typ licencií s parametrami, ktoré uchádzač navrhuje použiť ako súčasť svojej predkladanej ponuky. Budúcim vlastníkom všetkých dodávaných licencií bude MV SR.

Zhotoviteľ musí odovzdať obstarávateľovi zdrojové kódy aplikácií (vo forme umožňujúcej ich znovu použitie, modifikáciu a obsahujúcej sémantické metainformácie jednotlivých častí kódu), ktoré budú vyvinuté v rámci dodávky a autorské a licenčné podmienky nesmú zabraňovať riadnemu narábaniu so systémom pre neobmedzené množstvo používateľov a rozširovaniu systému podľa potrieb obstarávateľa.

Súčasťou všetkých uskutočnených zásahov do systému pred nasadením do produkčnej prevádzky, pri ktorých dôjde k zmene zdrojového kódu, zhotoviteľ poskytne obstarávateľovi tieto zmeny zdrojového kódu na dátovom nosiči vrátane súvisiacej dokumentácie.

### Podpora a údržba prevádzky

V rámci podpory a prevádzky systému Obstarávateľ požaduje od zhotoviteľa poskytovanie prevádzkovej podpory a údržby systému počas trvania zmluvy o NFP, t.j. do konca roku 2023.

Lehota na poskytovanie prevádzkovej podpory začína plynúť dňom podpísania Akceptačného protokolu po ukončení pod fázy Pilotná prevádzka.

Rozsah poskytovanej podpory bude uvedený v zmluve o Poskytovaní servisnej podpory, ktorá bude podpísaná s úspešným uchádzačom, a ktorej návrh je prílohou k Súťažným podkladom. Zmluva o Poskytovaní servisnej podpory bude uzatvorená so zhotoviteľom na obdobie 5 (piatich) rokov.

V rámci prevádzkovej podpory a údržby sa požaduje poskytovanie servisných služieb v zodpovedajúcej kvalite zaisťujúcej správnu, spoľahlivú a bezpečnú prevádzku Systému. Servisnými službami sa pre účel zmluvy rozumie podpora produkčnej prevádzky a zaistenie údržby Systému. Zhotoviteľ bude podporovať prevádzku systému HSM as a Service a Službu transparentného šifrovania po dobu 5 rokov.

Systém musí byť schopný prevádzky s dostupnosťou najmenej 99.5% (nerátajú sa plánované odstávky a výpadky infraštruktúry), pokiaľ konkrétny modul nemá uvedené iné požiadavky na dostupnosť, resp. podporu.

Požadovaný rozsah podpory:

* Riešenie technických a bezpečnostných incidentov,
* Prispôsobenie systému a optimalizačné úpravy na základe zákazníckych požiadaviek v rozsahu 10 človekodní mesačne, poskytovanie konzultácií
* Aplikácia opravných patchov
* Monitorovanie prevádzky

Rozsah plnenia štandardnej podpory pre riešenie technických incidentov:

* Servisný čas 24x7
* Reakčná doba 2 h
* Doba vyriešenia 1 d

Doba vyriešenia sa vzťahuje, len na technickú konfiguráciu a problémy s nastaveniami služieb.

Technické chyby hardware a software sú v plnej kompetencií výrobcu s nasledovnou SLA.

* Servisný čas 24x7
* Reakčná doba 2 h
* Výmena zariadenia Nasledujúci deň odoslanie nového zariadenia

Rozsah plnenia štandardnej podpory pre riešenie bezpečnostných incidentov:

* Servisný čas 24x7
* Reakčná doba 4 h

Pre bezpečnostné incidenty sa nedefinuje doba vyriešenia incidentu.

### Integrácia s CSP portálom Vládneho Cloudu

Vstupným portálom do prostredia Vládneho Cloudu je CSP portál na vyžiadanie si služby dodávanej Vládnym Cloudom. CSP portál je nutné integrovať s novými službami s dorazom na čo najväčšiu mieru automatizácie. Obstarávateľ preto požaduje od budúceho dodávateľa nasledovné:

* Plánovať náklady na integráciu s CSP portál a to na strane dodávateľa CSP portálu a aj na strane budúceho dodávateľa služby HSM as a service a služby centrálneho manažmentu kľúčov.
* Plánovať náklady na projektových manažérov
* Vytvorenie dokumentácie na strane oboch zainteresovaných dodávateľov
* Popis a vytvorenie automatizačných postupov v rámci riešenia.
* Spoločné odovzdanie funkčného diela objednávateľovi
* CSP portál bude riadiť jednosmerne požadovanú automatizáciu. To znamená, že po vyplnení formulárov na CSP portáli, CSP portál bude volať predpripravené workflows (REST API, SSH scripts, a pod.)

#### Očakávaná funkcionalita od integrácie HSM s priamym prístupom s CSP portálom

Na Portáli CSP by si koncový zákazník mal možnosť objednať a konfigurovať nasledovné služby:

* Vytvoriť vlastnú partíciu na konkrétnom fyzickom HSM
* Pri objednávaní viacerých partícií, partície by mali byť distribuované medzi viaceré fyzické HSM
* Po pred vytvorení partícií zákazník obdrží inštalačné súbory, a prvotné meno a heslo a stručný návod pre prispôsobenie svojej partície / vytvorenie clustra medzi partíciami, vytvorenie vlastných RW a R užívateľov.
* Nahratie vlastných verejných kľúčov asymetrickej šifry pre jednoznačnú identifikáciu klientov (server / PC)
* Zadefinovať klienta (server/pc), ktorý má mať prístup do ktorej partície

#### Očakávaná funkcionalita pre HSM s centrálnou službou manažmentu kľúčov a transparentného šifrovanie

Na Portali CSP si koncový zákazník môže definovať, či má záujem o vytvorenie vlastného tenant admina alebo ponechať správu tokenov v automatickom móde.

Pre obe možnosti je nutné prostredníctvom CSP portálu:

* Objednanie typu licencií pre jednotlivé funkcionality transparentného šifrovania (VM, Disk, FileSystem, Databáza, Štruktúrované dáta, Tokenizácia, ...)
* Objednanie počtu licencií pre jednotlivých klientov využívajúcich rôzne typy licencií
* CSP portál musí strážiť počty a využiteľnosť jednotlivých licencií.

Pri možnosti vlastného tenant admina:

* Prostredníctvom CSP portálu vytvorenie vlastného tenanta.
* V danom prostredí bude vytvorený nový tenant a cez CSP portál budú poskytnuté prihlasovacie údaje k management software, ako aj dokumentácia
* Licencie budú spravovane prostredníctvom CSP portálu.

Pri možnosti plne automatizovaného riešenia koncový zákazník musí prostredníctvom CSP portálu vedieť:

* Spravovať vlastné užívateľské účty
* Vytvárať si tokeny a priraďovať ich jednotlivým účtom
* Definovať si vlastné užívateľské skupiny
* Spravovať existujúce tokeny (revoke, rotation, ...)

### Bezpečnostný projekt

Od zhotoviteľa požadujeme zdokumentovanie bezpečnostných opatrení v bezpečnostnom projekte služby HSM as a Service ako celku.

Požadujeme, aby bezpečnostný projekt jasne vymedzil rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na systém služby HSM as a Service z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Bezpečnostný projekt musí spĺňať požiadavky vyplývajúce z:

* Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
* Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* Zákon 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Tento zákon upravuje ochranu práv fyzických osôb pred neoprávneným spracúvaním ich osobných údajov, práva, povinnosti a zodpovednosť pri spracúvaní osobných údajov fyzických osôb, postavenie, pôsobnosť a organizáciu Úradu na ochranu osobných údajov Slovenskej republiky.

Bezpečnostný projekt pre systém HSM as a Service a služby transparentného šifrovania musí obsahovať nasledovné časti (výstupy):

* Bezpečnostný zámer
* Analýza bezpečnosti služieb HSM a služby transparentného šifrovania
* Závery vyplývajúce z bezpečnostného zámeru a analýzy bezpečnosti (bezpečnostné smernice).

V rámci návrhu riešenia požadujeme vykonanie analýzy bezpečnostných rizík, z ktorej vyplynú podrobné nároky na bezpečnostné opatrenia. Tie požaduje implementovať najmä v priebehu fázy implementácia a testovania bezpečnostných opatrení, kedy budú vypracované aj prevádzkové postupy súvisiace s informačnou bezpečnosťou.

Bezpečnostný projekt ISVS je zameraný na naplnenie nasledovných požiadaviek:

* sumarizovať požiadavky vyplývajúce z legislatívy a iných záväzných predpisov týkajúce sa informačnej bezpečnosti ISVS a zdokumentovať ich naplnenie,
* navrhnúť technické, organizačné a personálne opatrenia potrebné na minimalizovanie hrozieb a rizík pôsobiacich na ISVS z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti,
* určiť rámec pre technické, organizačné a personálne opatrenia potrebné na minimalizovanie hrozieb a rizík pôsobiacich na ISVS a jednotlivé jeho časti z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti,
* spracovať vyhodnotenie komplexného riešenia a pokrytia rizík bezpečnosti ISVS
* splniť bezpečnostné ciele ISVS.

# Všeobecné požiadavky

Uchádzač v časti „Vlastný návrh riešenia“ popíše návrh svojho riešenia okrem vyplnenia preddefinovaných tabuliek aj vlastným textom minimálne v zmysle požiadaviek definovaných v tomto dokumente.

## Legislatívne požiadavky na riešenie

Tab. 3.1 Legislatívne požiadavky na riešenie

|  |  |
| --- | --- |
| **ID požiadavky** | **Požiadavka** |
| R 3.1.1 | Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti |
| R 3.1.2 | Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z |
| R 3.1.3 | Vyhláška č. 85/2020 Z.z., o riadení projektov, Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. |
| R 3.1.4 | Zákon č. 95/2019 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov |
| R 3.1.5 | Vyhláška č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy |
| R 3.1.6 | Zákon č. 18/2018 Z. z. o ochrane osobných údajov |
| R 3.1.7 | Súlad so štandardami pre informačné systémy v MV SR |
| R 3.1.8 | Splnenie kritérií na informačné systémy verejnej správy podľa strategickej priority strategickej priority Vládny Cloud |
| R 3.1.9 | Súlad do Zmluvou a Všeobecnými podmienkami pre poskytovane služieb dátových centier štátu |
| R 3.1.10 | Systém musí rešpektovať aktuálne európske nariadenia o ochrane osobných údajov (GDPR) |
| R 3.1.11 | Dodržanie zásad a politiky informačnej bezpečnosti MV SR |
| R 3.1.12 | Súlad s Referenčnou architektúrou ISVS pre cloud |

## Architektonické požiadavky

**Pri návrhu riešenia musia byť dodržané princípy:**

Uchádzač popíše architektúru navrhovaného riešenia pre služby HSM as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania.

Tab. 3.2 Požiadavky na dodržiavanie architektonických princípov

|  |  |
| --- | --- |
| ID požiadavky | Požiadavka |
| R 3.2.1 | Podpora rozširovanie podľa možností Vládneho Cloudu, pre zabezpečenie služby HSM as a service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania |
| R 3.2.2 | Popis architektúry multi-tenant riešenia a nastavenie partícií v rámci HSM a Služby centrálneho manažmentu kľúčov a transparentného šifrovania. |
| R 3.2.3 | Architektúra automatizácie v riešený HSM as a service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania |
| R 3.2.4 | Design HA riešenia formou active/active v rámci jedného datacentra. V rámci tohto projektu plánujeme s dvoma datacentrami. |
| R 3.2.5 | Prepojenie na existujúci Vládny Cloud a jeho služby a automatizačné moduly ako CSP a ICO |
| R 3.2.6 | Minimalizovanie administratívnej záťaže a úkonov klienta |
| R 3.2.7 | Používateľské rozhranie bude intuitívne, prehľadné, s dostupnou nápoveďou |
| R 3.2.8 | Využitie existujúcej funkcionality Vládneho Cloudu - IaaS MV SR. |
| R 3.2.9 | Design a dodávanie výkazov zo služby |
| R 3.2.10 | Definícia use case pre riešenie SIEM |
| R 3.2.11 | Design a definícia prístupov pre tenantov a administrátorov |

### Uplatnenie EA architektonického rámca

EA rámec bude obstarávateľ uplatňovať v častiach venujúcich sa architektúre. Pri návrhu architektúry obstarávateľ očakáva rámec ArchiMate 2.0 a vyšší.

### Stavebné bloky architektúry

Architektonický rámec slúži na znázornenie základnej organizačnej logiky riešenia.

.

* **Dátová architektúra** – popisujúca dátové štruktúry, ktoré sú spracovávané informačnými systémami počas prevádzkových procesov tak, aby boli naplnené a monitorované prevádzkové zámery.
* **Technologická architektúra** – musí zachytávať základnú štruktúru informačného systému z pohľadu hardvérových, softvérových a sieťových technológii a ich vzájomných vzťahov a vzťahu k prostrediu, popisuje aj princípy, ktoré riadia návrh a rozvoj systému.

### Ďalšie požiadavky na architektúru riešenia

Zároveň zhotoviteľ v prípade požiadavky poskytne obstarávateľovi súčinnosť pri evidencii dodaného riešenia v systéme MetaIS v súlade s aktuálnymi metodickým pokynom na aktualizáciu obsahu centrálneho meta informačného systému verejnej správy povinnými osobami“.

## Požiadavky na Bezpečnosť

Bezpečnosť a ochrana osobných údajov sú kľúčovými prvkami akéhokoľvek informačného systému, a preto je dôležité, aby ponuka služby HSM as a Service poskytovala vhodné schopnosti na zabezpečenie potrebnej bezpečnosti nasadeného riešenia.

## Projektové požiadavky

### Projektové riadenie

Požaduje sa splnenie nasledovných požiadaviek:

Zadávateľ požaduje od uchádzača manažment projektu počas celej doby trvania projektu, teda od nadobudnutia účinnosti Zmluvy o dielo až po odovzdanie a prebratie služby HSM as a Service všetkých jeho súčastí a modulov do produkčnej prevádzky.

Riadenie projektu musí prebiehať v súlade s výnosu č. 78/2020 Z. z. o štandardoch pre informačné systémy verejnej správ.

Zadávateľ požaduje od uchádzača opísať vo svojej ponuke metódu projektového riadenia, ktorú úspešný uchádzač použije pri implementácii aktivít. Uchádzač vo svojej ponuke popíše princípy projektového riadenia, zohľadní požiadavky na dodávku dokumentov projektového riadenia a životného cyklu projektu, ktoré vzniknú v rámci projektového riadenia a opíše spôsob a zodpovednosti rolí na všetkých nim navrhovaných pozíciách riadenia projektu.

Riadenie projektu musí byť v súlade s Aktualizovanou metodikou projektového riadenia projektov informatizácie verejnej správy (vyhláška č. 179/2020 Z. z.).

### Dokumenty projektového riadenia

V rámci plánovania projektu zhotoviteľ pripraví nasledujúce dokumenty pre oblasť projektového riadenia a to v nasledujúcich fázach:

|  |  |  |  |
| --- | --- | --- | --- |
| **Názov dokumentu** | **Fáza** | **Zodpovednosť** | **Forma výstupu** |
| Definícia projektu | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Projektový plán s úplným zoznamom dodávok dodávateľa a projektovými míľnikmi (harmonogram projektu) | Plánovanie Projektu | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Organizačná štruktúra projektu s popisom rolí a zodpovedností | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Komunikačný plán | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Komunikačná matica | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| RACI MATRIX | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Projektový tím | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Správa o stave projektu | priebežne, v každej etape podľa schváleného komunikačného plánu | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Správa pre Riadiaci výbor | priebežne, v každej etape podľa schváleného komunikačného plánu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Plán riadenia rizík a problémov | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Register rizík | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Zoznam riešených problémov | priebežne, v každej etape podľa stavu projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Zoznam požiadaviek na zmenu | priebežne, v každej etape podľa stavu projektu | zadávateľ/zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Plán pre riadenie konfigurácie | Plánovanie Projektu | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Zoznam produktov a ich stav | priebežne, v každej etape podľa stavu projektu | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Správa o ukončení fázy a projektu | pred koncom etapy, resp. projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Plán zabezpečenia kvality produktov | Plánovanie Projektu | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Plán zabezpečenia kvality riadenia projektu | Plánovanie Projektu | zhotoviteľ/zadávateľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Plán súčinností zadávateľa | s odhadom prácnosti a typu súčinnosti pre každú fázu; pred koncom aktuálnej etapy | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Schvaľovací protokol pre akceptáciu fázy | pred koncom aktuálnej etapy | zhotoviteľ | Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |
| Bezpečnostný projekt | Realizačná fáza projektu | zhotoviteľ | Dokument obsahuje Analýzu rizík,  Bezpečnostnú politiku, bezpečnostnú stratégiu a zálohovacie plány a plány obnovy  Forma výstupu: Nástroj MS Office alebo ekvivalentné opensource nástroje (XLS, DOC, PDF,...) |

Je požadované, aby dokumenty pripravené vo fáze Plánovanie projektu boli schválené obstarávateľom a to pred začiatkom práce nasledujúcej fázy projektu.

V rámci ďalších fáz je možné dané dokumenty aktualizovať, resp. doplnenia, pričom tieto zmeny podliehajú schváleniu projektovým manažérom zadávateľa.

Iné zmeny do schválených dokumentov sú možné až po schválení obstarávateľom projektu.

Zhotoviteľ je povinný nedostatky/pripomienky v dokumentoch v dohodnutej primeranej lehote (s ohľadom na Časový harmonogram) zapracovať a odstrániť.

Štruktúra jednotlivých dokumentov podlieha schváleniu zo strany zadávateľa.

### Záruka na všetky komponenty služby HSM as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania.

Objednávateľ požaduje poskytnutie záruky na akosť dodaných služieb a tovarov na obdobie 24 mesiacov odo dňa podpisu preberacieho protokolu.

Objednávateľ požaduje poskytnutie záruky na softvér a hardware, jeho všetky spôsoby aktualizácie ako aj služby súvisiace s uvedením softvéru a hardware do produkčnej prevádzky v produkčnom prostredí objednávateľa pri rešpektovaní všetkých funkčných a nefunkčných požiadaviek.

Objednávateľ neočakáva upgrade hardware komponentov počas trvania kontraktu.

Objednávateľ požaduje od zhotoviteľa v prípade uplatnenia reklamácie reklamovanú chybu alebo chýbajúcu funkčnosť bez zbytočného odkladu odstrániť alebo sprevádzkovať chýbajúcu funkcionalitu.

V prípade, že sa v záručnej dobe prejaví porucha  bude požadované vykonanie servisného zásahu na základe podmienok podľa kapitoly  2.4.9. Podpora a údržba prevádzky.

# Detailné požiadavky na predmet zákazky

### Úrovne služieb Hardware Secure Module (HSM) as a Service a Služby centrálneho manažmentu kľúčov a transparentného šifrovania – služby Vládneho Cloudu

Služba HSM by mala poskytovať podporu pre aplikácie a systémy od tých z nízkou až po vysokú kritickosť s dorazom na dostupnosť služby.

Požadovaná štandardná podpora pre produkčné prostredie:

* Servisný čas - 24x7
* Reakčná doba – 2 h
* Doba vyriešenia – 1 d

Doba vyriešenia sa vzťahuje, len na technickú konfiguráciu a problémy s nastaveniami služieb.

Technické chyby hardware a software sú v plnej kompetencií výrobcu s nasledovnou SLA.

* Servisný čas 24x7
* Reakčná doba 2 h
* Výmena zariadenia Nasledujúci deň odoslanie nového zariadenia

**Tabuľka Dostupnosti služby HSM as a Service**

|  |  |  |  |
| --- | --- | --- | --- |
| Názov | Popis | Dostupnosť a fyzické umiestnenie | Servisná podpora  Servisný čas[[1]](#footnote-1)  Reakčná doba[[2]](#footnote-2)  Doba vyriešenia incidentu[[3]](#footnote-3) |
| Tier 1 | Tier 1 predstavuje najvyššiu úroveň z pohľadu dostupnosti a je charakterizovaný viac uzlovým nasadením služby (za pohľadu optimálnej dostupnosti 1 a viac uzlov), pričom samotná implementácia môže byť realizovaná replikáciami, HA A-A, HA A-P klastrami, a podobne. z pohľadu nasadenia je služba rozprestretá na viac geografických lokalít. | 99,9 %  DC Kopčianska a DC Tajov | **Štandardná podpora**  Servisný čas - 24x7  Reakčná doba – 2 h  Doba vyriešenia – 1 d |

HSM as a Service služba musia byť navrhnuté, pripravené tak, aby mohla splniť SLA typu Tier1.

## Požiadavky na Multi-tenantnú službu HSM s priamym prístupom pre Key Management a PKI

Pre služby vládneho cloudu sa predpokladá, že budú využívať možnosti služieb Hardware Secure Module (HSM) as a Service – služby vládneho cloudu pre interné potreby a pre potreby iných organizácií, ktoré budú mat možnosť konzumovať služby vládneho cloudu. Služba HSM as Service postavená na základe general purpose HSM, ktoré je schopné vykonávať viacero funkcionalít. Tak isto je možné ho použiť na šifrovanie, dešifrovanie údajov, generovanie kľúčov a podpisu v podobe digitálnej signatúry.

Dôležitou funkcionalitou Služby HSM as a Service je funkcionalita viacerých nájomcov zariadenia HSM (Multi-tenant). Keďže sa jedná o cloudovú službu, tato funkcionalita je kritická. Je nevyhnutne potrebné mat možnosť zdieľať HSM zariadenia až do počtu 100 separátnych partícií per HSM pre Tenantov., ktoré majú potrebu konzumácie HSM služby. Každý Tenant bude mať možnosť si spravovať vlastnú partíciu a v nej zadefinovane nastavenia. Každý Tenant má možnosť objednať si viacero partícií.

Ďalšou nevyhnutnou funkcionalitou je škálovateľnosť riešenia. To znamená možnosť rýchleho rozšírenia existujúceho hardware riešenia o ďalšie komponenty. V rámci tejto požiadavky sa jedná len o sieťové HSM zariadenia.

Hardware Secure Module (HSM) as a Service – služby Vládneho Cloudu musí spĺňať nižšie uvedené funkčné požiadavky.

Tab. 4.5. Funkčné vlastnosti modulu:

|  |  |
| --- | --- |
| ID požiadavky | Požiadavka |
| R 4.5.1 | Podpora multiplatform (windows, linux, aix, solaris) |
| R 4.5.2 | Služba bude dostupná len vo forme Network HSM. |
| R 4.5.4 | Knižnice pre vývojove prostredia .Net (CSP,CNG), Java jsp, PKCS#11 |
| R 4.5.5 | Funkcionalita vzdialeného reštartu, bez nutnosti byt fyzicky prítomný v datacentre. |
| R 4.5.6 | Certifikácia na úrovni FIPS-140-2 Level3 alebo zodpovedajúcej, uznáva sa aj certifikácia samotného HSM modulu sieťového zariadenia a MFA , číže Password a Multi-Factor Autentifikáciu (PED) |
| R 4.5.7 | Funkcionalita zdieľaného HSM, avšak s dedikovanou partíciou, ktorá je oddelená od ostatných partícii, bez možnosti prístupu a zamenenia. |
| R 4.5.8 | Funkcionality Access Controll List (ACL) pre dáta v rámci partície, ktorá však nemusí byt FIPS/CC certifikovaná |
| R 4.5.9 | Pre redundantné riešenie je potrebné mat dostupnú funkcionalitu active/active alebo Active/pasive. |
|  | Design HA riešenia formou active/active v ramci jedného datacentra. V rámci tohto projektu plánujeme s dvoma datacentrami. |
| R 4.5.10 | Riešenie musí podporovať integráciu HSM služby v rámci datacentier služby Vládneho Cloudu so službou HSM as a service výrobcu HSM produktov. |
| R 4.5.11 | Podpora dvojfaktorovej autentifikácie na prístup k dátam v rámci HSM služby. |
| R 4.5.12 | Podpora Rest API na prístup k HSM zariadeniam / partíciám. |
| R 4.5.13 | Možnosť bezpečnej blokácie obsahu/ konfigurácie pri nutnom presune zariadenia medzi datacentrami Vládneho Cloudu MVSR |
| R 4.5.14 | Podpora bezpečnostného logovania pre potreby auditu. |
| R 4.5.15 | Bezpečnostné zálohovanie HSM nastavenia |
| R 4.5.16 | HSM zariadenie musí byt tamper proof. To znamená chránene voči fyzickému prístupu k dátam. |
| R 4.5.17 | Podpora operačných systémov virtualizácie a to VMware, Hyper-V, Xen a KVM. |
| R 4.5.18 | Nutnosť podpory asymetrického šifrovania a to nasledovné:  RSA, DSA, Diffie-Hellman,  Šifrovanie na báze eliptických kriviek ECDSA, ECDH, Ed25519, ECIES. |
| R 4.5.19 | Nutnosť podpory asymetrického šifrovania a to nasledovné:  AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST |
| R 4.5.20 | Nutnosť podpory šifrovania Full Suite B |
| R 4.5.21 | Podpora protokolov SNMP a Syslog nazbieranie Log informácií |
| R 4.5.22 | Podpora funkcionality hot swap pre elektrické zdroje |
| R 4.5.23 | Podpora bezpečnostných štandardov a podpora súladu s environmentálnymi štandardami ako sú UL, CSA, CE, FCC, CE, VCCI, TAA |
| R 4.5.24 | Hardware HSM komponenty musia byt vyhotovených v rozmeroch pre rýchlu a štandardnú inštaláciu v rámci Rackou Vládneho Cloudu ministerstva Vnútra Slovenskej republiky. Štandardne sa uvádza 19” appliance. |
| R 4.5.25 | HSM fyzický hardware musí podporovať IPv4 a IPv6 protokoly. |
| R 4.5.26 | Fyzický hardware musí obsahovať minimálne 2x 10Gbps optické porty a 2x 1Gbps porty na jednom HSM zariadení. |
| R 4.5.27 | Podpora vysokého výkonu a to až do 8 700 a viac transakcií za sekundu pri podpore šifrovania RSA-2048 na jednom samostatnom HSM zariadení. Tak isto je podporovaný do 14 000 a viac transakcií za sekundu v prípade kryptografie na báze eliptických kriviek (ECC). |
| R 4.5.28 | HSM zariadenie ako General purpose HSM musí obsahovať funkcionality podpisu dokumentov |
| R 4.5.29 | HSM zariadenie ako General purpose HSM musí obsahovať funkcionality podpisu kódu |
| R 4.5.30 | HSM zariadenie ako General purpose HSM musí obsahovať funkcionality podpisu a validácie PKI certifikátov |
| R 4.5.31 | HSM zariadenie ako General purpose HSM musí obsahovať funkcionalitu šifrovanie databázy |
| R 4.5.32 | HSM as a service musí obsahovať funkcionalitu split of responsibility, kde pre operátorov je možné zadefinovať k akým častiam a funkcionalitám HSM budú mat prístup |
| R 4.5.33 | HSM as a service služba musí byt registrovaná a konzumovateľná v rámci služieb Vládneho Cloudu MVSR. |
| R 4.5.34 | HSM as a Service musí byt integrovateľná so službou bezpečnostného monitoringu. |
| R 4.5.35 | Podpora bezpečnej likvidácie HSM hardware |
| R 4.5.35 | Podpora definície viacerých rolí pre Administrátorov služby HSM as Service. |
| R 4.5.36 | Podpora funkcionality Load Balancing |
| R 4.5.37 | Možnosť zamknúť HSM v rámci Racku |
| R 4.5.38 | Funkcia Display na hardware HSM, ktorý bude poskytovať základne informácie ohľadne zabezpečenia, software verzie a informáciách o sieťovom pripojení. |
| R 4.5.39 | Funkcionalita zdvojenia elektrických zdrojov na HSM zariadení (2xHot Swap Power Supplies) |
| R 4.5.40 | HSM riešenie musí byť inštalované separátne pre každé datacentrum. |
| R 4.5.41 | Riešenie musí mať aspoň 10 logických partícií a musí byť licenčne rozšíriteľné na vytváranie min. 100 logických partícií na ukladanie kryptografického materiálu s nezávislou správou a overovaním a úplným oddelením navzájom |
| R 4.5.42 | Poskytnutie fyzickej a logickej ochrany kryptografických kľúčov.  Riadenie prístupu ku kryptografickým kľúčom  Akcelerácia operácií s využitím kryptografických kľúčov |
| R 4.5.43 | Minimálne 22000 podpisov ECC P256 za sekundu  Minimálne 17000 AES-GCM small packet encryption transakcií za sekundu. |
|  | **Licencovanie** |
| R 4.5.44 | Licencie/Subskripcie musia byť na obdobie min. 3 roky |
| R 4.5.45 | 2x Hardwarové apliance HSM veľkosti 1U zapojená v HA  HW musí byť vo vyhotovení pre inštaláciu do štandardizovanej 19" skrine, max. výška 1U, s dvoma nezávislými napájacími zdrojmi s možnosťou výmeny počas behu zariadenia |

## Požiadavky služieb Centrálneho manažmentu kľúčov a Transparentného Šifrovania s využitím HSM na správu kľúčov. – služby Vládneho Cloudu

Pre služby vládneho cloudu sa predpokladá, že budú využívať možnosti služieb centrálneho manažmentu kľúčov a transparentného šifrovania pre interné potreby a pre potreby iných organizácií (tenantov), ktoré budú mat a majú možnosť konzumovať služby vládneho cloudu. Služba transparentného šifrovania je postavená na službe šifrovania Data at rest s centrálnym manažmentom kľúčov a funkciou auditných logov prístupu. Služba transparentného šifrovania na ochranu dát v cloude, lokálnej infraštruktúre alebo kontajnerovom prostredí. Tak isto umožňuje šifrovanie pre technológiu IBM AIX (Power9).

Ďalšou nevyhnutnou funkcionalitou je škálovateľnosť riešenia. To znamená možnosť rýchleho rozšírenia existujúceho hardware riešenia o ďalšie komponenty.

Keďže sa nachádzame v cloudovom prostredí Ministerstva vnútra je dôležité, aby služba podporovala Multi-tenant funkciu, aby každý zákazník zadávateľa mal možnosť správy vlastných kľúčov.

Služba Transparentného šifrovania – služby Vládneho Cloudu musí spĺňať nižšie uvedené funkčné požiadavky.

Tab. 4.6. Funkčné vlastnosti modulu:

|  |  |
| --- | --- |
| ID požiadavky | Požiadavka |
| R 4.6.1 | Funkcia šifrovania súborov na cieľovom systéme |
| R 4.6.2 | Riešenie musí podporovať operácie naprieč viacerými nasadeniami a produktmi šifrovania a zároveň zabezpečiť, aby správcovia mali obmedzené role definované pre ich rozsah zodpovednosti z konzoly centralizovanej správy.  KMS musí využívať existujúce adresáre LDAP alebo AD na mapovanie administratívneho a kľúčového prístupu pre aplikáciu a koncových používateľov (integrované aplikácie) |
| R 4.6.3 | Podpora operačných systémov Microsoft server 2012/2016 a 2019, Linux a IBM AIX (Power9) |
| R 4.6.4 | Podpora databázových systémov MySql, Oracle, NoSQL, MicrosoftSQL server, IBM DB2 |
| R 4.6.5 | Podpora Big Data ako napríklad MangoDB, Sap Hana, Hadoop, Cloudera, IBM NoSQL |
| R 4.6.6 | Podpora šifrovania na procesoroch AMD, Intel AES-NI a IBM P9 kryptograficky processor |
| R 4.6.7 | Certifikácia agenta transparentného šifrovania na FIPS 140-2 Level 1 |
| R 4.6.8 | Transformácia údajov bez výpadku. Je požadovaná funkcionalita šifrovania počas chodu databázy, systému, bez nutnosti zastavenie systému pre proces šifrovania alebo výmeny kľúčov |
| R 4.6.9 | Podpora silných šifrovacích protokolov, ako je AES (Advanced encryption standard) pre šifrovanie dát. |
| R 4.6.10 | Podpora silných šifrovacích protokolov na výmenu kľúčov postavenej na báze eliptických kriviek (Elliptic Curve Cryptography-ECC) |
| R 4.6.11 | Detailný audit log o prístupe k dátam šifrovaným produktom pre transparentné šifrovanie |
| R 4.6.12 | Integrácia so službou SIEM |
| R 4.6.13 | Funkcia Web konzoly, rest API a CLI pre manažment služby transparentného šifrovania |
| R 4.6.14 | Možnosť implementácie manažmentu ako virtuálny alebo fyzický appliance. |
| R 4.6.15 | Manažment certifikácia- v súlade s FIPS 140-2 |
| R 4.6.16 | Funkcia integrácie so službou HSM na správu kľúčov |
| R 4.6.17 | Funkcionalita High Availability pre manažment služby transparentného šifrovania |
| R 4.6.18 | Funkcia tokenizácie aj s Data maskingom |
| R 4.6.19 | Funkcia šifrovania štruktúrovaných dát v databáze. |
| R 4.6.20 | Šifrovanie celých virtuálnych systémov s uloženými kľúčmi na HSM a manažment cez centrálny manažment transparentného šifrovania. Riešenie musí podporovať vSphere a vCenter. |
| R 4.6.21 | Systém musí byť schopný integrácie s hardvérovým bezpečnostným modulom (HSM) certifikácie FIPS 140-2 Level3 alebo vyššou na ochranu šifrovacích kľúčov.  • Riešenie musí byť schopné uložiť najmenej 1.000.000 kryptografických kľúčov  • Riešenie musí podporovať viac serverov a aplikácií z viacerých umiestnení v sieti. Toto riešenie musí byť schopné podporovať až 100 000 pripojení súčasne  • Riešenie by malo umožňovať vzdialenú správu cez WebUI, CLI a REST API.  • Systém KMS musí poskytovať integráciu prostredníctvom nasledujúcich rozhraní API / rozhraní: NAE-XML, KMIP, REST API, PKCS#11, JCE,.NET,MSCAPI, MS CNG, NAE-XML  Riešenie by malo ponúkať možnosti správy kľúčov, ktoré je možné integrovať do rôznych komerčných šifrovacích produktov. Podporované technológie musia obsahovať:  šifrovanie aplikácií (integrácia cez API),  šifrovanie databázy vrátane natívneho šifrovania databázy (napr. transparentné šifrovanie údajov dostupné v serveroch MS SQL Server a Oracle Database),  riešenia šifrovania na úrovni súborov a úložísk  výrobky podporujúce štandard protokolu OASIS Key Management Interoperability Protocol (KMIP), |
| R 4.6.22 | Funkcia PKCS#11 v rámci služby centrálneho manažmentu kľúčov |
| R 4.6.23 | Flexibilné Licencovanie postavené na type systému, ktorý treba transparentne šifrovať a od počtu koncových klientov, ktorý majú byť šifrovaný. |
| R 4.6.24 | Systém musí ponúkať možnosti správy kryptografických kľúčov počas ich životného cyklu vrátane generovania kľúčov, importu a exportu kľúčov a rotácie kľúčov.  Všetky kryptografické kľúče musia byť uložené v centralizovanom, spevnenom virtuálnom zariadení, aby sa zjednodušila správa a zaistila prísna bezpečnosť.  Podpora redundancie HA (High availability) |
| R 4.6.25 | Systém musí byť schopný vykonávať minimálne tieto operácie :  - správa šifrovacích kľúčov počas celého životného cyklu  - generovať symetrické a asymetrické kryptografické kľúče, ako aj tajné údaje a certifikáty X.509  - distribúcia kľúčov, deaktivácia a vymazanie  - automatizované operácie založené na policies musia zjednodušovať úlohy vypršania platnosti a rotácie kľúčov  - zabezpečiť kontrolu prístupu ku kľúčom  - zálohovanie a obnova kryptografického obsahu a konfigurácie |
| R 4.6.26 | KMS je možné nasadiť v klastrovanej konfigurácii s replikáciou kľúčov, zásad a konfiguračných informácií v reálnom čase vo viacerých inštanciách - čo umožňuje úplné zotavenie po katastrofe a kontinuitu podnikania.  KMS s dodávaným softvérom musia byť schopné pracovať v režime vysokej dostupnosti.  V prípade viacerých riešení šifrovania integrovaných do KMS musia byť kľúče spravované centrálne bez toho, aby to malo citeľný vplyv na výkon systému. |
| R 4.6.27 | Riešenie musí umožňovať zálohovanie a obnovu kryptografického obsahu a konfigurácie  Zálohovanie musí byť chránené (aspoň pomocou prístupovej fázy).Riešenie musí vykonávať zálohy na požiadanie a podľa harmonogramu |
| R 4.6.28 | Kryptografický modul KMS musí umožňovať podrobné logovanie a sledovanie auditu všetkých kľúčových zmien stavu, prístupu správcu a zmien zásad.  Protokoly auditu musia byť bezpečne uložené a podpísané, aby sa nedali odmietnuť, a môžu byť poskytnuté s nástrojmi SIEM tretích strán prostredníctvom syslogu.  Alarmy sú mechanizmom na upozorňovanie správcov, keď stav KMS alebo niektorého z jeho uzlov nie je v poriadku alebo nie je nakonfigurovaný bezpečne a mali by sa preskúmať.  Riešenie musí umožňovať nastavenie alarmu pre nasledujúce udalosti:  - Disk je plný  - NAE-XML TLS disabled  - HSM offline  - Cluster node down |
| R 4.6.29 | Licencie/Subskripcie musia byť na obdobie min. 3 roky |

# Akceptačné konanie

Výsledkom akceptačného konania môžu byť 2 (slovami: dva) stavy:

Akceptované. V prípade, že Objednávateľ v priebehu akceptačného konania nenájde v príslušnom plnení žiadne Vady, alebo budú v priebehu akceptačného konania nájdené Vady a to v počte 0 (slovom: nula) Vád. Pre každý dodávaný produkt samostatne, uvedie Objednávateľ do akceptačného protokolu, že poskytnuté plnenie bolo akceptované a akceptačný protokol potvrdí svojím podpisom (pre prípad, že plnenie bude mať Vady, musí akceptačný protokol tiež obsahovať lehoty odstránenia Vád Zhotoviteľom, na ktorých sa dohodnú Objednávateľ a Zhotoviteľ.

Neakceptované. V prípade, že budú v priebehu akceptačného konania v odovzdanom plnení zistené Vady a to v počte 1 (slovom: jedna) a viac závažných Vád, nie je plnenie akceptované a nie je tiež považované za poskytnuté v súlade so Zmluvou. Zmluvné strany sa dohodnú na termínoch nového odovzdania a nového akceptačného konania. V akceptačnom protokole bude uvedené, že poskytnuté plnenie nebolo akceptované a budú stanovené termíny nového odovzdania a akceptačného konania a Zmluvné strany akceptačný protokol potvrdia svojím podpisom.

Príslušné dodávky podľa Zmluvy je možné prevziať len na základe akceptačného konania s výsledkom "Akceptované".

## Metódy akceptácie

Akceptačné konanie vykonávané za účelom kontroly plnenia akceptačných kritérií sa bude vykonávať prostredníctvom nasledujúcich metód vykonávania akceptačných skúšok, pričom môže prísť aj ku kombinácii jednotlivých metód vykonávania akceptačných skúšok:

|  |  |
| --- | --- |
| **Metóda vykonávania akceptačných skúšok** | **Popis** |
| **Demonštrácia / Predvedenie** | Predvedenie je metóda vykonávania akceptačných skúšok, pri ktorej sa požadovaná dodávka za neúplných kontrolovaných podmienok predvedie alebo ukáže a tým sa potvrdí, že definovaná požiadavka/akceptačné kritérium bola/o splnená/é. Predvedenie sa nezameriava na hľadanie chýb, avšak dodávka musí byť v takom stave, aby mohla byť v plnej dohodnutej miere predvedená. |
| **Test** | Test je metóda vykonávania akceptačných skúšok, pri ktorej sa overenie požiadavky/splnenia akceptačného kritéria deje za úplných kontrolovaných podmienok. Testovanie je zamerané na odhaľovanie chýb dodávky pri stanovených podmienkach |
| **Analýza** | Analýza je metóda vykonávania akceptačných skúšok, pri ktorej na základe merania vybraných vzoriek systému alebo špecifických dát, možno pomocou analýzy  dokázať, že požiadavky/akceptačné kritériá sú splniteľné. Napríklad sa metóda analýzy môže použiť na požiadavky/akceptačné kritériá týkajúce sa kapacity alebo výkonnosti systému. Tiež sa metóda analýzy používa pri požiadavkách, ktoré sa úplne prejavia až počas používania systému. |
| **Simulácia** | Simulácia je metóda vykonávania akceptačných skúšok, pri ktorej sa použije špecifický súbor dát a vstupných parametrov a monitoruje sa správanie systému a očakávajú sa exaktné predpokladané simulované výsledky. Môže sa používať kombinácia reálneho systému spolu so simulátormi chýbajúcich komponentov (alebo komponentov, ktoré nie je možné v danom čase použiť. |
| **Inšpekcia** | Inšpekcia je metóda vykonávania akceptačných skúšok, pri ktorej prichádza k overeniu pomocou vizuálneho pozorovania, že požiadavka/akceptačné kritérium bola/o splnená. Môže sa použiť počas vývoja, taktiež napríklad pri školeniach vyhodnocovaním kvality prostredníctvom anketových formulárov. Rovnako sa môže použiť pre dokumenty ako report z testovania, rôzne certifikáty a iné špecifické dokumenty. |

Na akceptáciu dokumentov sa pre účely vykonania akceptačných skúšok použije metóda vykonávania akceptačných skúšok „Revízia dokumentácie“ a/alebo „Inšpekcia“. Konkrétny spôsob akceptácie príslušných dokumentov bude dohodnutý vopred najneskôr však 5 dní pred zahájením akceptácie na projektovej úrovni zodpovednými osobami zmluvných strán.

Na akceptáciu školení a pracovných poradných stretnutí (workshop) sa pre účely vykonania akceptačných skúšok použije metóda vykonávania akceptačných skúšok „Inšpekcia“.

Na akceptáciu prezentácií a služieb sa pre účely vykonania akceptačných skúšok použije metóda vykonávania akceptačných skúšok „Predvedenie“ a/alebo „Test“, a/alebo „Simulácia“. Hodnotenie, kontrola plnenia a akceptácia úrovne prebehne na základe akceptačného konania. Aký konkrétny spôsob bude pre ktorú službu použitý bude oboma zmluvnými stranami dohodnutý a schválený vopred najneskôr však 5 dní pred zahájením samotnej akceptácie jednotlivej služby na projektovej úrovni zodpovednými osobami zmluvných strán. Ak sa zmluvné strany nedohodnú, sa pre účely vykonania akceptačných skúšok použije metóda „Test“.

Na akceptáciu softvérových dodávok sa pre účely vykonania akceptačných skúšok použije po dohode oboch zmluvných strán najmä, nie však výlučne metóda vykonávania akceptačných skúšok „Test“ uskutočnený na základe vopred schválených/akceptovaných testovacích scenárov.

1. Doba počas ktorej je poskytovaná servisná podpora. [↑](#footnote-ref-1)
2. Doba do ktorej poskytovateľ cloudovej služby poskytne spätnú väzbu odberateľovi cloudových služieb. [↑](#footnote-ref-2)
3. Doba do ktorej musí byť incident vyriešený, alebo je poskytnuté náhradné riešenie. [↑](#footnote-ref-3)